2MP IPSN V4 Series IP Cameras

User manual

Models:

- DI-320IPSN-28-V4
- DI-320IPSN-28-G-V4
- DI-320IPSN-36-V4
- DI-320IPSN-VF-V4
- DI-320IPSN-MVF-V4
- DAI-320IPSN-28-V4
- I2-320IPSN-28-V4
- I4-320IPSN-28-V4
- I4-320IPSN-VF-V4
- I4-320IPSN-MVF-V4

Index

Index **1**

1) Terms & Conditions **3**

2) Camera Activation **5**

3) Remote Access **6**

3.1) LAN 6
3.1.1) Access through the IP Manager Tool 6
3.1.2) Direct Access through Web-Browser 7

3.2) WAN 8
3.2.1) Direct Access through IP/DDNS 8
3.2.2) Access through NAT/P2P 9

4) Live Preview **10**

4.1) Live View Interface 10

4.2) MVF (Motorized Vari-Focal) Controls* 11

5) IPC Configuration **11**

5.1) System Configuration 11
5.1.1) Basic Information 11
5.1.2) Date & Time Configuration 12

5.2) Local Config 13

5.3) Storage 13

5.4) Image Configuration 16
5.4.1) Camera Configuration 16
5.4.2) Video/Audio 18
5.4.3) OSD Configuration 19
5.4.4) Video Mask 20
5.4.5) ROI Configuration 20
5.4.6) Zoom/Focus* 20

5.5) Alarm Configuration 21
5.5.1) Motion Detection 21
5.5.2) General Fault 22
5.5.3) Alarm Server 23

5.6) Analytics 24
5.6.1) Camera Tampering 23
5.6.2) Line Crossing 24
5.6.3) Sterile Area 26

5.7) Network 27

5.7.1) TCP/IP 27
5.7.2) Port 28
5.7.3) Auto Report 29
5.7.4) ONVIF 29
5.7.5) DDNS 29
5.7.6) SNMP 30
5.7.7) 802.1X 30
5.7.8) RTSP 30
5.7.9) RTMP 31
5.7.10) UPnP 31
5.7.11) Email Setting 32
5.7.12) FTP 33
5.7.13) HTTP POST 33
5.7.14) HTTPS 34
5.7.15) P2P 35
5.7.16) QoS 35

5.8) Security 36
5.8.1) User 36
5.8.2) Online Users 37
5.8.3) Block and Allow Lists 38
5.8.4) Security Management 39
5.8.5) Check Point Protection 40

5.9) Maintenance 41
5.9.1) Configure Backup & Restore 41
5.9.2) Reboot Device 41
5.9.3) Upgrade 42

6) Playback 43

1) Terms & Conditions

- We strongly advise users to read this manual and keep it for later use for proper and safe device usage.

- Please use the provided & authorized by Provision-ISR technician power supply and power source indicated on the marking label. The power voltage must be verified before use.

- Avoid improper operation, shock vibration, and heavy pressing that can cause product damage.

- Do not use corrosive detergents when cleaning. When necessary, please use a soft dry cloth to wipe the dirt off; use neutral detergents for problematic pollution & decay. Any cleanser for high-grade furniture is applicable.

- Keep away from heat sources such as radiators, heat registers, stoves, etc.

- Do not try to repair the device without technical aid or approval.
- For camera installations:
- Avoid aiming the camera directly towards extremely bright objects, such as the sun, which may damage the image sensor.
- Please abstain from reversing the camera. This will result in an inverted image. Please follow the instructions for proper camera installation.
- Do not operate the camera in extreme temperatures or extreme humidity conditions.
- For Recorder & server installations:
- Do not block any ventilation openings and ensure proper airing around the device.
- Perform a safe shutdown before disconnecting from power. Otherwise, HDD damage and configuration loss might occur.
- This device is for indoor use only.
- Do not install this device near water, nor expose it to rainy or moist environments. If any solids or liquids get inside the device's case, turn the device off immediately and have it checked by a qualified technician.

- The instructions in this manual are suitable for all models running Ossia OS. Models which do not support any of the features will have explicit markings.

- For devices with internal power supply, please ensure that the AC 220/110V input selector is set correctly.

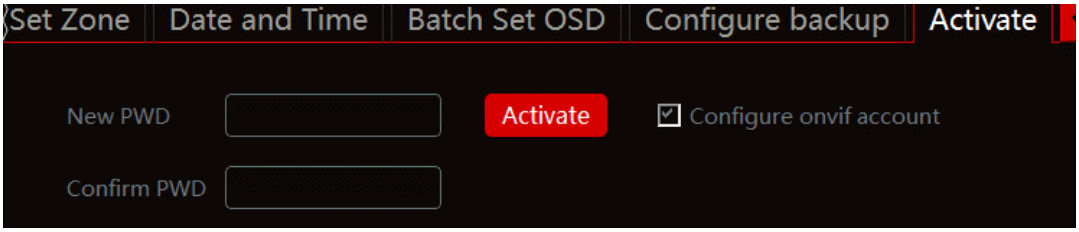
- There may be incorrect info or printing errors in this manual. PROVISION-ISR reserves the right to change this manual and publish the revision online on our website (www.provision-isr.com); there may be inconsistencies with the latest version, which apply to any software upgrades and product improvements, interpretation and modification added. Updates and corrections are subject to change without notice.

- All pictures and examples used in the manual are for reference purposes only.
- When this device is in use, the relevant contents of Microsoft, Apple and Google are involved. The ownership of trademarks, logos, and other intellectual properties related to Microsoft, Apple, and Google, belong to the companies mentioned above.

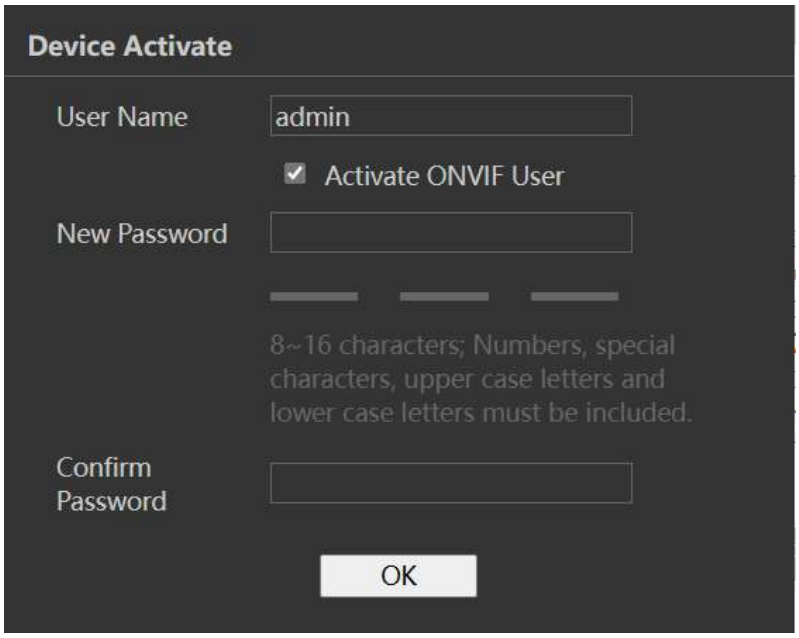
2) Camera Activation

The camera's default state is “Inactive”. This means that the camera must be activated before it can be used. The camera can be activated by 3 methods:

- IP Manager Tool: Select the camera(s) you wish to activate, set the new admin password and click activate (Note: the activation password must contain at least 8 characters and include 1 letter, 1 number, and 1 special character). After setting the password, you will have to set the answer to 3 recovery questions of your choice. These recovery questions can be used in case you have lost the admin password you have set.



- Logging into the camera web page: When browsing to the camera for the first time, you will be prompted to activate it. Use credentials admin/123456 for the first login, then you will be prompted to set the new admin password and click activate (Note: the activation password must contain at least 8 characters and include 1 letter, 1 number, and 1 special character).
  After setting the password, you will have to set the answer to 3 recovery questions of your choice. These recovery questions can be used in case you have lost the admin password you have set.



- Setting the camera on an NVR: NVRs running Firmware version >1.4.10 can activate the camera through their UI. Please refer to the NVR manual for details process.

3) Remote Access

Cameras running FW version >5.1.1 support all modern browsers (Chrome, Firefox, Safari, Opera, Edge), and can also work on Edge in IE mode.

3.1) LAN

In LAN, there are two ways to access IPC:

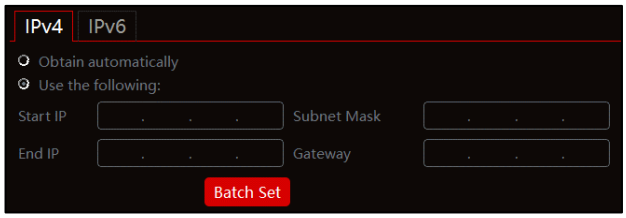
1. Access through IP Manager Software.
2. Direct access through IE browser.

3.1.1) Access through the IP Manager Tool

- ❖ Make sure the PC and IPC are connected to the LAN and that the IP Manager is installed on the PC. You can download the IP manager from here.
- ❖ Double-click the IP-Manager icon on the desktop to run this software.

- ❖ Modify the IP address. The default TCP/IP setting of this camera is set to DHCP so the address is not fixed. If no DHCP server is available on your network, the camera setting will change to "fixed IP" with the address 192.168.226.201. Tick all the cameras you wish to set and then click on the "Batch Set NET" tab.

If you wish to set static IP addresses, choose "Use the following IP Addresses", set the range of IP addresses you wish to assign (First and last address), set the gateway and subnet mask, and click on batch set. Wait for a few moments until the IP manager will configure the cameras. After configuration, the IP addresses of the cameras will refresh automatically.



Please note:

- ❖ The IP range must fit the number of chosen cameras.
- ❖ The selected IP addresses in the specified range must be available.

For example, if the IP address of your computer is 192.168.1.4, then the IP address of the cameras should be changed to 192.168.1.x. (x stands for any number between 1 and 255).

- Double-click on the IP address of the device you want to connect to. The system will automatically open a browser and connect to the IPC. A login window will appear as shown below.

Input the username and password to log in.

3.1.2) Direct Access through Web-Browser

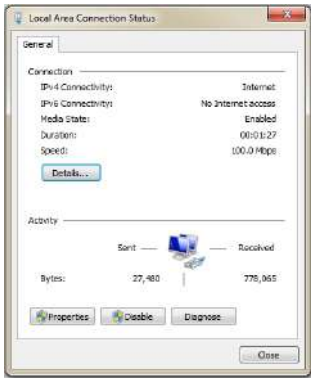
In case there is no DHCP server available in the network, the default network settings will be as shown below:

IP address: 192.168.226.201
Subnet Mask: 255.255.255.0
Gateway: 192.168.226.1
HTTP: 80
Data port: 9008

You may use the above default settings when you log in to the camera for the first time.

1. You can use the IP manager to access the camera even if the camera is still using the default IP address. Double-click on the IP address within the IP manager for the system to open your default web browser and browse to the camera. You can then set the IP address from the camera configuration menu.

2. If you wish to access the camera using its default IP address (192.168.226.201) you will have to manually set the IP address of the PC to be in the same IP segment as the default settings of the IP camera. Open the network and sharing center. Click “Local Area Connection” to pop up the following window.



Select “Properties” and then select internet protocol according to the actual situation (most probably you are using IPv4). Next, click on the “Properties” button and set the network of the PC as shown on the right.

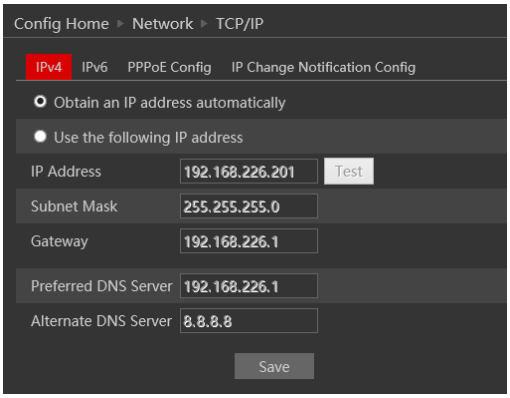
Open your preferred web browser, input the IP address of IPC and confirm. Input the default username and password and click “Login”.

3.2) WAN

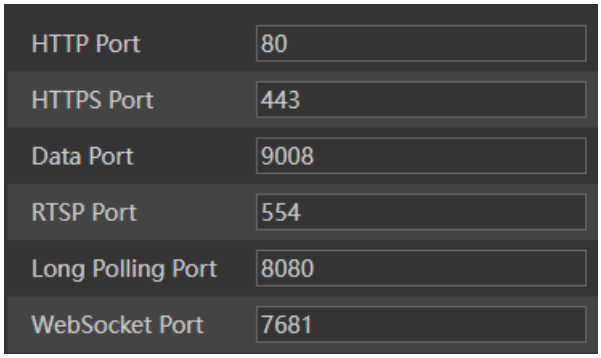
3.2.1) Direct Access through IP/DDNS

Allows you to access the camera using a router or virtual server.

1. Make sure the camera is well connected and configured via LAN. Log in to the camera via LAN and go to the Config→Network Config→Port menu to set up the port number.
2. Go to Config→Network Config→TCP/IP menu to modify the IP address.
3. After modifying the IP Address, click on “Port” and modify the port according to your needs.



IP Setup



Port Setup

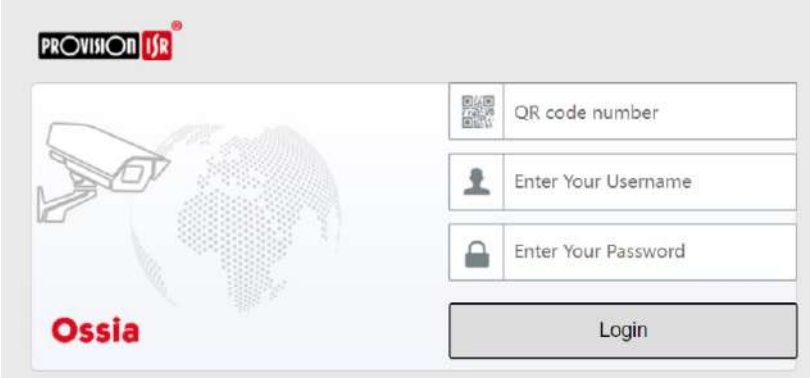
4. Go to the router’s management interface through your browser to forward the IP address and port of the camera to the “Virtual Server”. In the picture example below, you will see an example of the setting as if the IPC IP address is “192.168.6.6” and the ports are default (9008 & 80)

Default Ports:
HTTP Port (Default is 80) is for HTTP and API
Data Port (Default is 9008) is for IE video data and SDK
WebSocket Port (Default is 9681) is for modern browser video streaming

3.2.2) Access through NAT/P2P

P2P allows indirect connection to the camera without the need for port forwarding and virtual server triggers on the router.

1. Enable P2P (Please refer to chapter Network→P2P for more information)
2. Browse to http://www.provisionisr-cloud.com to the following interface



Input the QR code number, user name, and password, then click on "Login"

Please note:

- The QR code number can be found under settings→System→Basic Information.
- P2P Connection is only supported via IE Web browser (Or Edge on IE mode)
- P2P Connection offers limited features/configuration than direct IP/DDNS connection

4) Live Preview

4.1) Live View Interface

Icons and operation buttons:

Icon	Description	Icon	Description
	Actual Video Size		Digital Zoom-Out
	Fit to screen – True Proportions		MVF Controls*
	Fit to screen - Stretch	/	Check Point IoT protection Enabled/Disabled
	Full-screen	/	Motion Detection indicator
/	Enable/Disable live view		SD Card recording indicator
	Talk	/	Alarm In Indicator
	Listen	Main stream	Use mainstream for live-view
	Take Snapshot	Sub stream	Use sub-stream for live-view
	Enable/Disable Local Recording	Third stream	Use third stream for live-view
	Digital Zoom-in	Balanced	Choose the buffering plan

Please note:

❖ There might be deviations between available icons on different IPC models

4.2) MVF (Motorized Vari-Focal) Controls*

Clicking on the MVF lens controls will unfold the MVF control panel. Using this interface, you can control the zoom and focus of the MVF lens.

The descriptions of the control panel are as follows:

Icon	Description	Icon	Description
	Zoom Out		Focus In
	Zoom In		One Key Focus
	Focus Out		

*Relevant for MVF Models Only

5) IPC Configuration

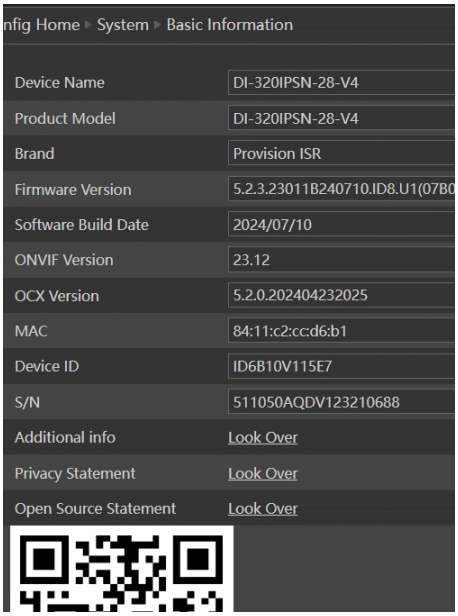
In this chapter, we will go through all the possible configurations of the IPC.

5.1) System Configuration

The “System Configuration” includes four submenus: Basic Information, Date & Time, Local Config, and Storage.

5.1.1) Basic Information

In the “Basic Information” interface, you can view all the necessary information related to the IPC, as seen on the right:



The following table will explain the available detail field.

Parameter	Explanation
Device name	Name of the device – can be modified from the OSD settings
Product Model	The model of the device
Brand	The brand of the camera
Software version	The current software version
Software build date	The software build-date
ONVIF Version	The current ONVIF version
S/N	Device serial number
MAC	The MAC address of the device
Device ID and QR	QR Code used for P2P connection

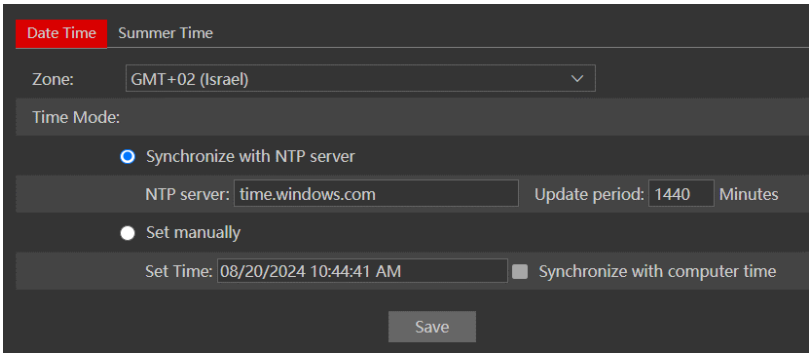
Additional information can be found when clicking on “About this machine”. The relevant details are below

Parameter	Explanation
Hardware version	The hardware identifier of the device
Kernel version	The kernel version of the device
Video Structured version	The AI engines version on the current firmware

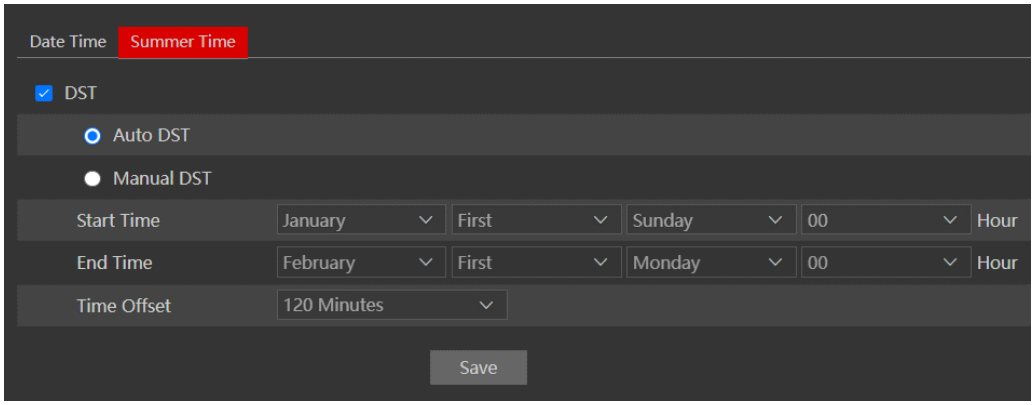
5.1.2) Date & Time Configuration

Setting steps:

1. Go to Config→Date & Time menu as shown below.

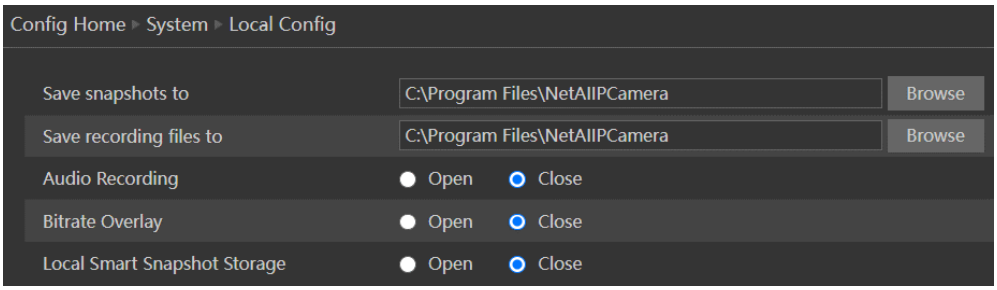


2. Set the time zone.
3. Set the time and date. You may synchronize the camera time with an NTP server and set the NTP time correction intervals (Internet connection required), synchronize the camera time with the time of the computer you are using, or set the time manually.
4. Go to the “Time Zone” tab to set DST.
5. Enable DST mode if required. DST settings are already configured according to your time zone. If you wish to set the DST manually, switch to “Manual DST” and set it accordingly.



5.2) Local Config

Go to "System Configuration" →"Local config" as shown below:



From here you can set the path on your computer where local snapshots and videos will be saved.
You can also choose if the camera will show the current bit-rate on the live-view image (Local interface only).

5.3) Storage

The SD card feature allows you to insert an SD card into the camera and enable the camera to operate with local storage. The SD card will be used for both snapshot and video files. You can allocate a certain percentage for each from the settings menu.Go to "System Configuration" →"Storage"

5.3.1) SD Card Settings

If it is the first time you are using the SD card with the camera or if the state is showing any value different than "Normal", you should click on "Format" before the SD card will be available for recording.
Click "Eject card" to stop writing data to the SD card and allow you to remove it safely. Inserting an SD card into the camera must be done while the camera is powered off.

Please note:

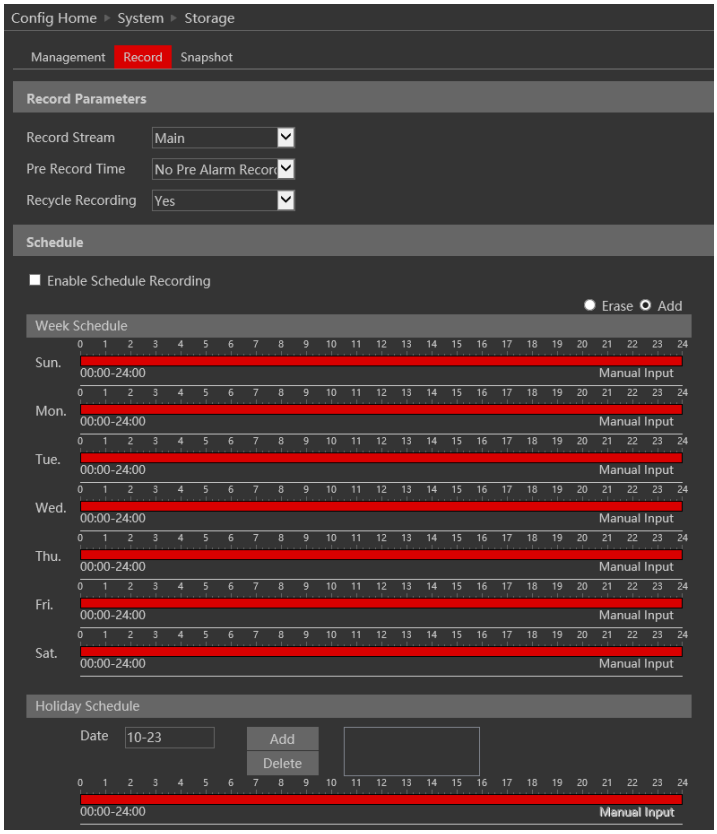
- Removing the SD card while the camera is working without using the "Eject" button, will corrupt all the record data and make it unusable.

The following table will explain the available detail fields.

Parameter	Meaning
Total picture capacity	The total capacity dedicated to pictures (Snapshots)
Picture remaining space	Available capacity for pictures (Snapshots)
Total recording capacity	The total capacity dedicated to video records
Recording remaining space	Available capacity for video records
State	The state of the SD card.
Snapshot Quota	The percentage of the SD card dedicated to Snapshots
Video Quota	The percentage of the SD card dedicated to Videos

5.3.2) Record Setting

The next tab is “Record”. Click on it to set the video recording parameters and schedule.



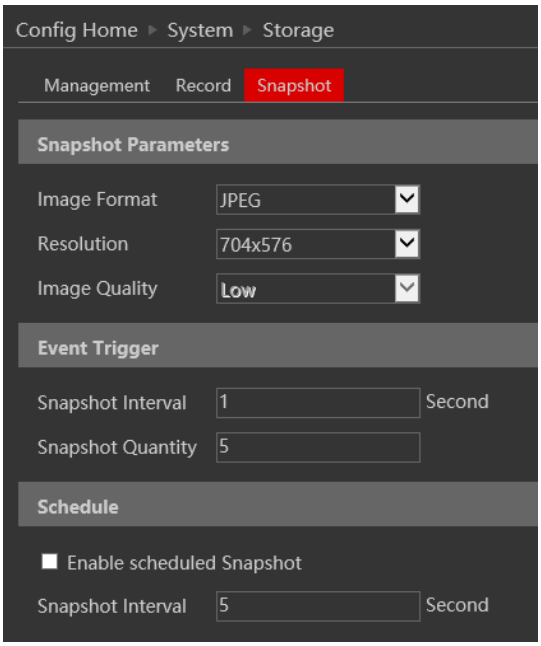
The video parameters are as follows:

Parameter	Meaning
Record stream	Which video stream will be used to record
Pre-recording time	The duration of the video before the recording trigger
Cycle recording	Whether to recycle the record or stop when the SD card is full

Below are the schedule settings. Enable the schedule if required and set the recording time for each of the weekdays. You can also set a holiday schedule and add the required dates to it.

5.3.3) Snapshot Setting

The next tab is “Snapshot” Click on it to set the snapshot parameters and schedule.



The snapshot parameters are as follows:

Parameter	Meaning
Image Format	The image format is JPEG
Resolution	Set the snapshot resolution
Image quality	The quality of the image reflects its size.
Snapshot Interval	The duration between two snapshots
Snapshot Quantity	The total number of snapshots to be taken after a trigger
Scheduled snapshots	Taking a snapshot according to a specified schedule

Below are the schedule settings. Enable the schedule if required and set the recording time for each of the weekdays. You can also set a holiday schedule and add the required dates to it.

5.3.4) FTP Snapshot Setting

The FTP Snapshot setting is used to send a snapshot to a configured FTP server on a set interval.

Select the FTP server you want to send the snapshot to, and the snapshot interval (In seconds. The range is 1 second to 86400 seconds (Which equivalents to a 1 snapshot per day)

Please note:

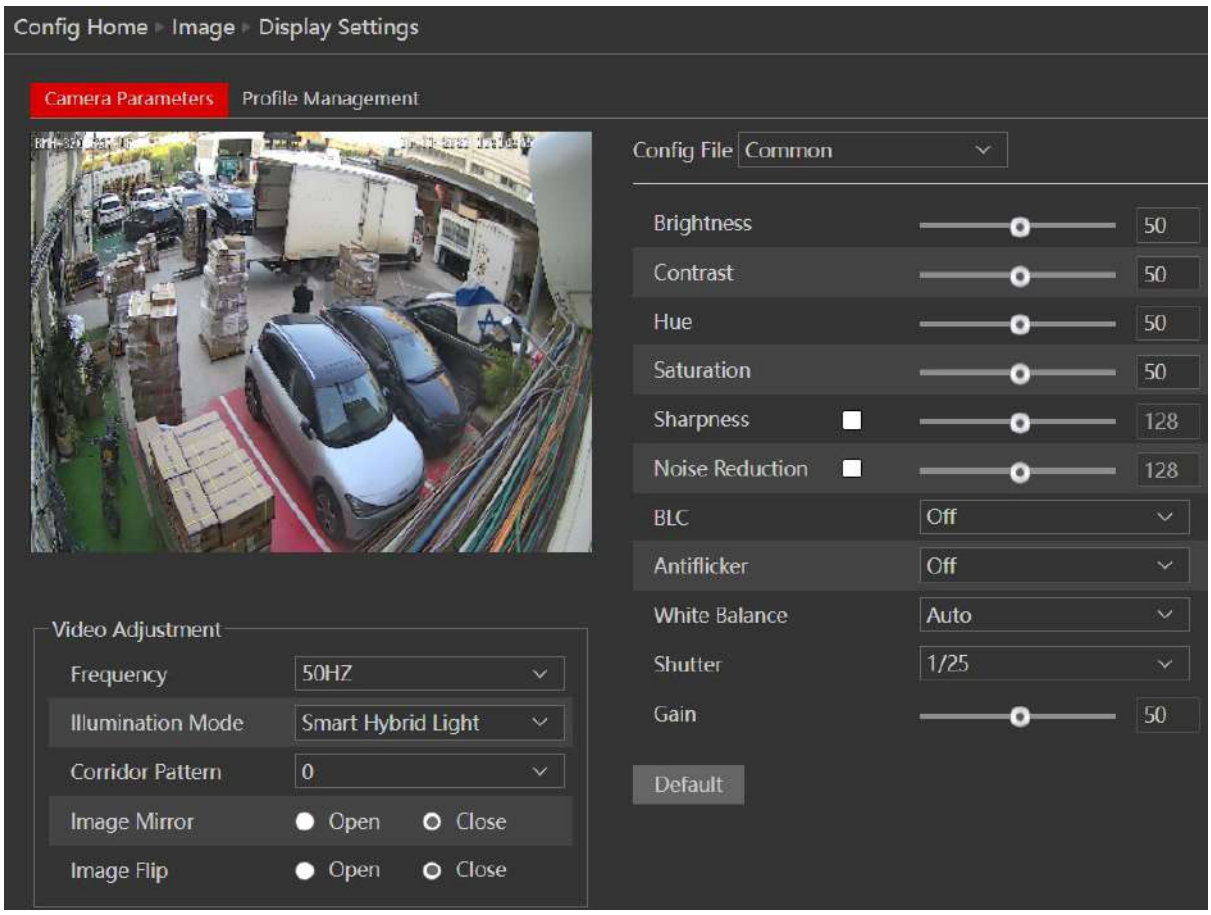
- You must configure an FTP server via Settings→Network→FTP before being able to successfully set the FTP Snapshots

5.4) Image Configuration

Image Configuration includes five submenus: Display Settings, Video/Audio Stream, OSD Config, Video Mask, and ROI Config.

5.4.1) Camera Parameters

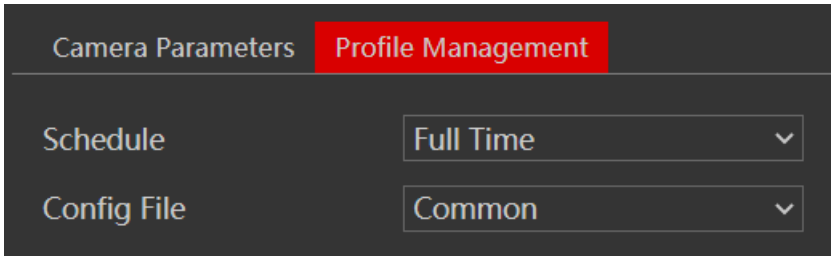
Setting steps:
Go to "Display Settings" → "Display" interface as shown below.



The display parameters are as follows:

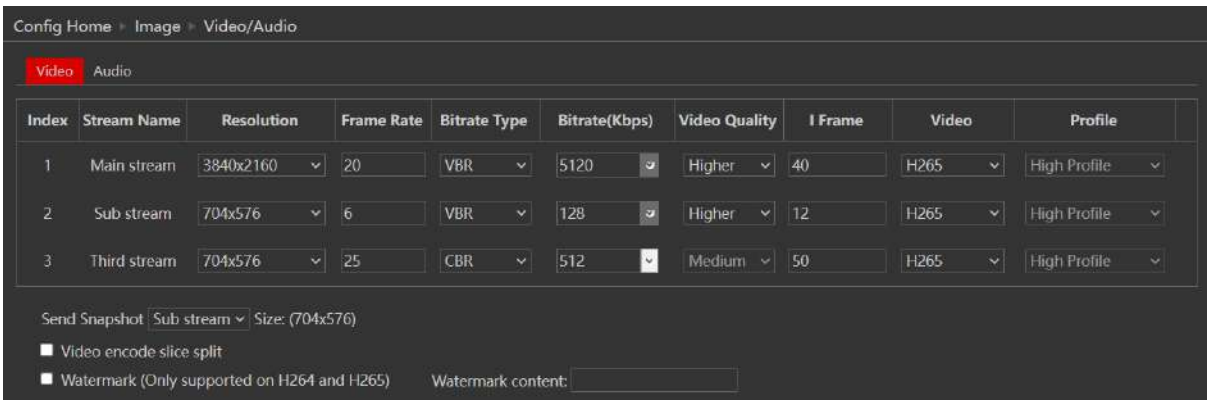
Parameter	Meaning
Config file*	You can set an individual configuration for Day and night. Common is used for both
Brightness	Set the image brightness
Contrast	Set the image contrast
Hue	Set the image hue
Saturation	Set the image saturation
Sharpness	Enable/Disable the sharpness and set its level
Noise reduction	Enable/Disable the 3D-DNR and set its level
Defog	Enable/Disable the defog and set its level
BLC	Set HLC/BLC/True-WDR to deal with advanced light conditions.
Level	The Level of the HWDR/BLC/HLC
Antiflicker	Changes the camera refresh rate to reduce flickers
Smart-IR	Enable Smart IR function that prevents burnt pixels due to strong IR illumination.
White Balance	Set the white balance of the camera
Day/Night Mode*	Set the day/night mode (Auto/Day/Night/Schedule)
Sensitivity	The light sensor sensitivity
Delay Time	The delay time before switching day/night modes
Shutter Mode	Set the exposure to auto or set it manually
Max.	Maximum allowed shutter speed
Gain Mode	Set gain to Auto/Manual
Gain Limit	Set the Gain limit
Frequency	Set the frequency to 50/60Hz
Illumination Mode	Set the Illumination light (IR, White LED, Hybrid)
Corridor Pattern	Rotate the image to fit corridors
Image Mirror	Mirror the image horizontally
Image Flip	Flip the image vertically

*If you set the day/night mode to schedule or you wish to differentiate between the daytime and night-time image settings, you will need to set the profiles accordingly. Click on the “Profile Management” tab and set the schedule as you wish.



5.4.2) Video/Audio

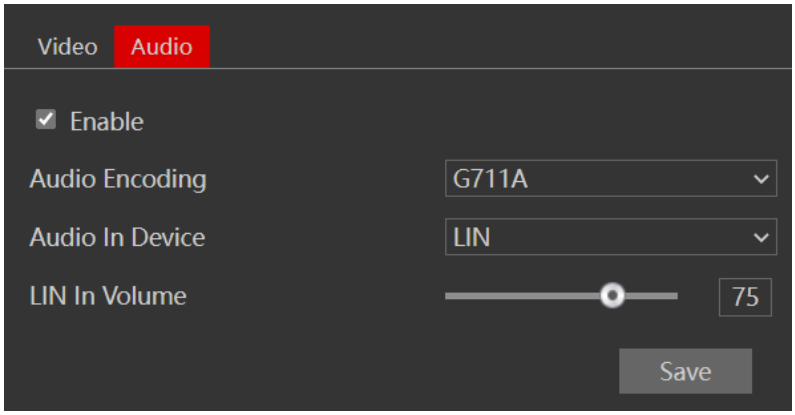
Go to “Video configuration” → “Video/Audio” to see an interface as shown below.



Three video streams are available. You can set each one of them differently with the limitations of the camera’s capabilities.

Parameter	Meaning
Resolution	The higher the resolution is, the bigger the image is.
Frame rate	The higher the frame rate is, the more fluent the video is. However, more storage room will be taken up.
Bitrate type	CBR (Constant Bit-Rate) means that the video compression bitrate will be constant as configured. This will not only facilitate the image quality better in a constant bitrate but also help to calculate the capacity of the recording. VBR (Variable Bit-Rate) means that the compression bitrate can be automatically adjusted according to the change of the video resources with the configured bit-rate as the maximum value. This will help to optimize the storage network bandwidth.
Video Quality	When VBR is selected, you need to choose image quality. The higher the image quality you choose, the more bitrate will be required.
Bitrate	Please set it according to your needs while taking into consideration the bandwidth and storage limits.
I Frame interval	It is recommended to use the default value. If the value is too high, the read speed picture group will be slow resulting in video quality loss.
Video Compression	Choose between H.265 and H.264. The IPC also supports MJPEG on sub-stream resolution but you need to make sure that the application connected to the camera also supports it.
Profile	Baseline, main profile, and high profile are optional. A baseline profile is mainly used in interactive applications with low complexity and delay. The main or high profile is mainly used for higher coding requirements.
Send Snapshot	Please select it according to the actual situation.
Video encode slice split	If enabled, you may get a more fluent image even when using a low-performance PC.
Watermark	You can set a watermark that will appear on the image.

In the next tab, we have “Audio” settings as shown below:



The audio input / built-in microphone is disabled by default. Enable it if you need audio input from the camera.
Set the encoding profile as desired and the type of audio input. If LIN (Line) is selected, it means that the audio input is already amplified and the input volume will be set to “low”. If MIC (Microphone) will be selected, it means that the audio signal is not amplified and the input volume will be set to “high”.

5.4.3) OSD Configuration

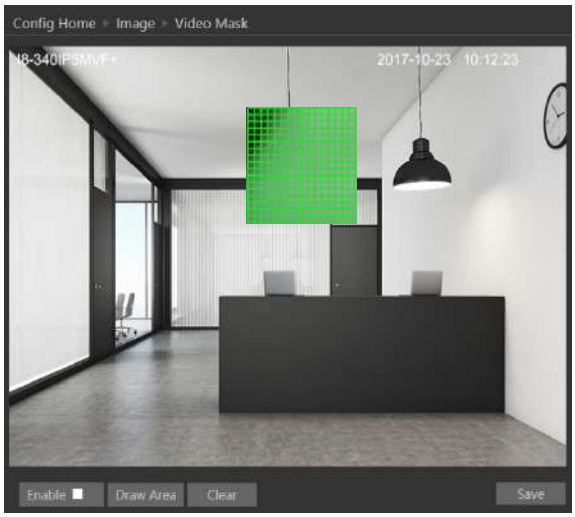
Go to “Image” → “OSD” menu to display the interface as shown below.
You may set the device name, timestamp, and custom OSDs here. Drag the time stamp and custom OSD over the image on the left side to set their position. Then press the “Save” button to save the settings.

5.4.4) Video Mask

A video mask is used to cover areas that should be censored from the video images.
You can set 4 mask areas at most.

To set up a video mask

1. Enable video mask.
2. Click the "Draw" button and then drag the mouse to draw the video mask area.
3. Click the "Save" button to save the settings.
4. Return to the live view to see the following picture.



To clear the video mask:

Go to the video mask menu and then click the "Clear" button to delete the current video mask area.

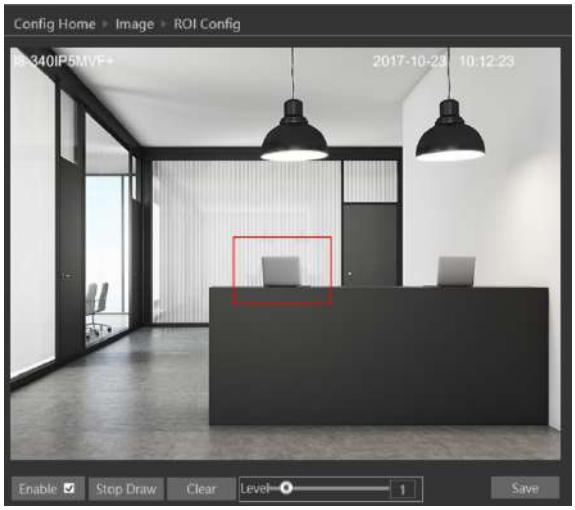
5.4.5) ROI Configuration

ROI is used to allocate a higher bit-rate on a certain area of the image than other areas

To set up ROI

1. Go to Config→ROI menu.
2. Check "Enable" and then click the "Draw" button.
3. Set the level.
4. Click the "Save" button to save the settings.

Now, you will see that the selected ROI area is clearer than other areas, especially in low bit-rate settings.



5.4.6) Zoom/Focus*

The zoom/focus interface is used for setting the lens of the camera (In MVF Models only).
You can also enable "Day/Night Switching focus" which will refocus the lens every time the camera switched from day to night and vice-versa.

"One Key Focus" will automatically focus the lens in one click.

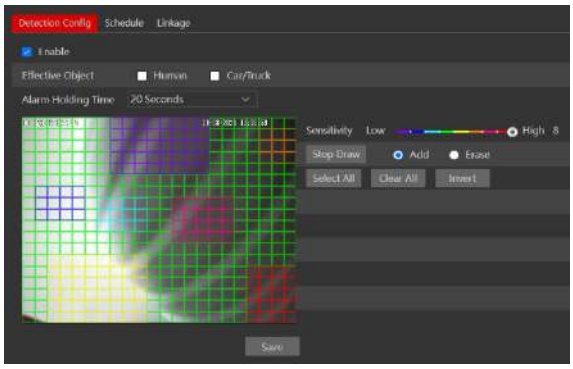
Zoom +/- will manually control the zoom ratio.
Focus +/- will manually set the focus of the lens.

5.5) Alarm Configuration

Alarm configuration includes four submenus: Motion Detection, General Fault, and Alarm Server.

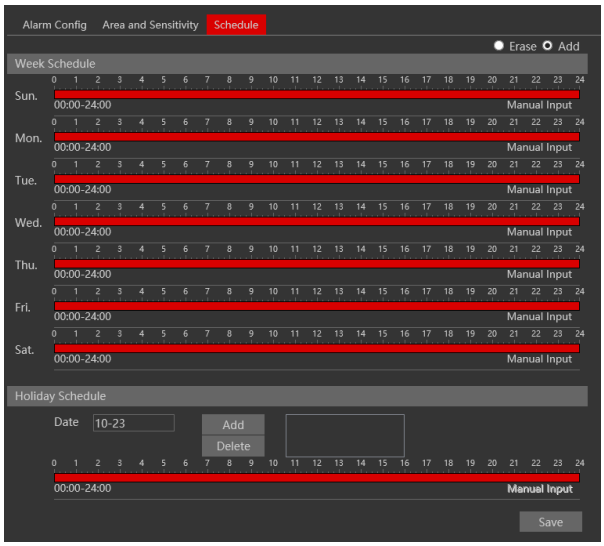
5.5.1) Motion Detection

Go to “Alarm configuration”→ “Motion Detection”

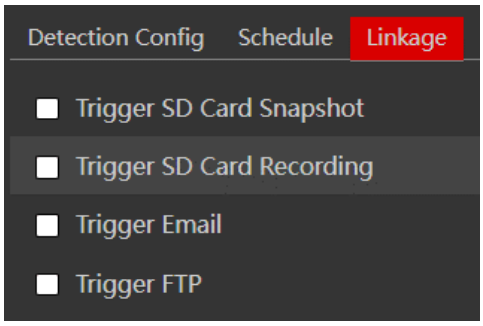


Enable or disable the alarm. Move the “Sensitivity” scroll bar to set up the motion sensitivity and click on “draw” to enable the marking on the image. Note that you can set different sensitivities to a different area of the picture as shown below. Once finished, click on “Stop Draw”.
If needed you can refine the motion detection by enabling SMD. Do so by choosing weather to only detect Humand, vehicles or both.
Set the alarm holding time. The holding time means that the alarm signal will stay active and no additional alarms will be generated during that time.

Next is the “Schedule” tab:
Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add the required dates to it.



Choose the camera’s response to the alarm in the linkage tab as explained below:



Alarm Triggers:	Explanation:
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

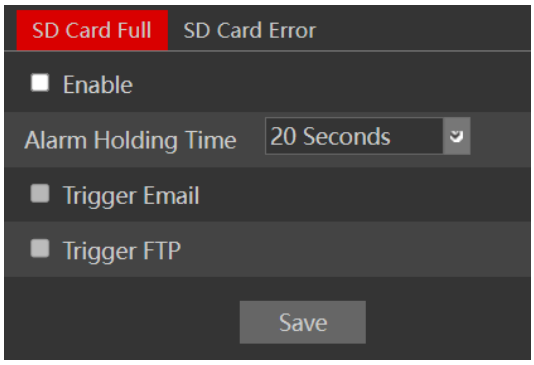
4. Click “Save” to save the settings.

5.5.2) General Fault

A problem with the network cable or with the SD card will produce a general fault. The alarms can be configured as follows: SD Card Full, SD Card Error, IP Address Conflict, Network cable disconnected.

Enter “Alarm Configuration”→ “General Faults” to see a screen as shown below. The default tab is “SD Card Full”:

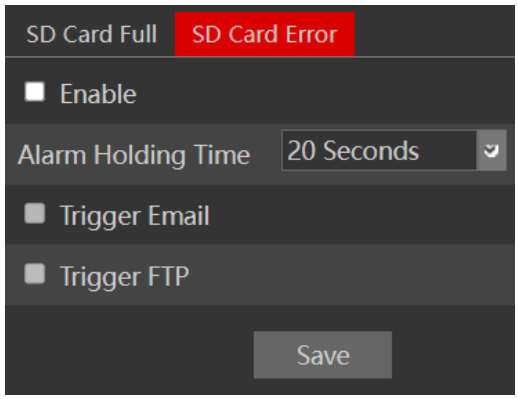
Enable the alarm if required. This alarm will only be relevant if the “Recycle Record” is not marked. If the “recycle record” is active, the SD card will not trigger an event once the card is filled.



After enabling the alarm, choose the responses required from the camera in case the alarm will be active. After the setting is complete, click “Save”.

Next is the “SD Card Error” Tab. This alarm will be triggered if any fault will be developed with the SD card. It can be a malfunction or removing the SD card from the camera.

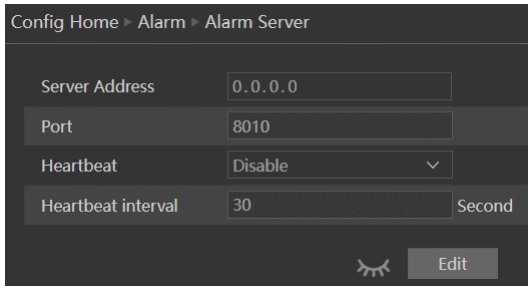
To activate it, enable the alarm.



After enabling the alarm, choose the responses required from the camera in case the alarm will be active. After the setting is complete, click “Save”.

5.5.3) Alarm Server

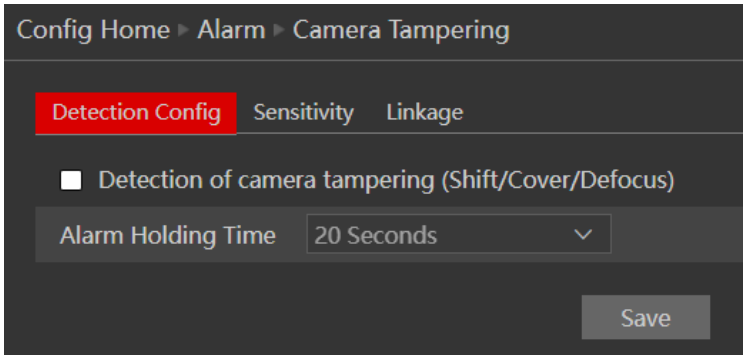
Alarm server is used mainly for system integrations. Once enabled, the camera will send all events to a dedicated listening server. These events will be sent in an XML format that needs to be parsed by the server. If required, a heartbeat can be set to confirm that the server that the camera is working and has network connectivity to it.



5.5.4) Camera Tampering

Camera tapering uses a special analytics algorithm to detect if the camera was tampered with. This analytics detects if the camera was shifted from its original location, covered or that the lens was tampered with.

1. Go to "Analytics"→ "Camera Tampering" to get to the interface as shown below:



2. Enable the alarm if required and set the alarm holding time. The holding time means that the alarm signal will stay active and no additional alarms will be generated during that time.
3. Go to the sensitivity tab:

4. Set the sensitivity (0 – lowest, 100 – Highest)
5. Set the Alarm response as follows:

Alarm Triggers:	Explanation:
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

6. Click "Save" to confirm.

5.6) Analytics

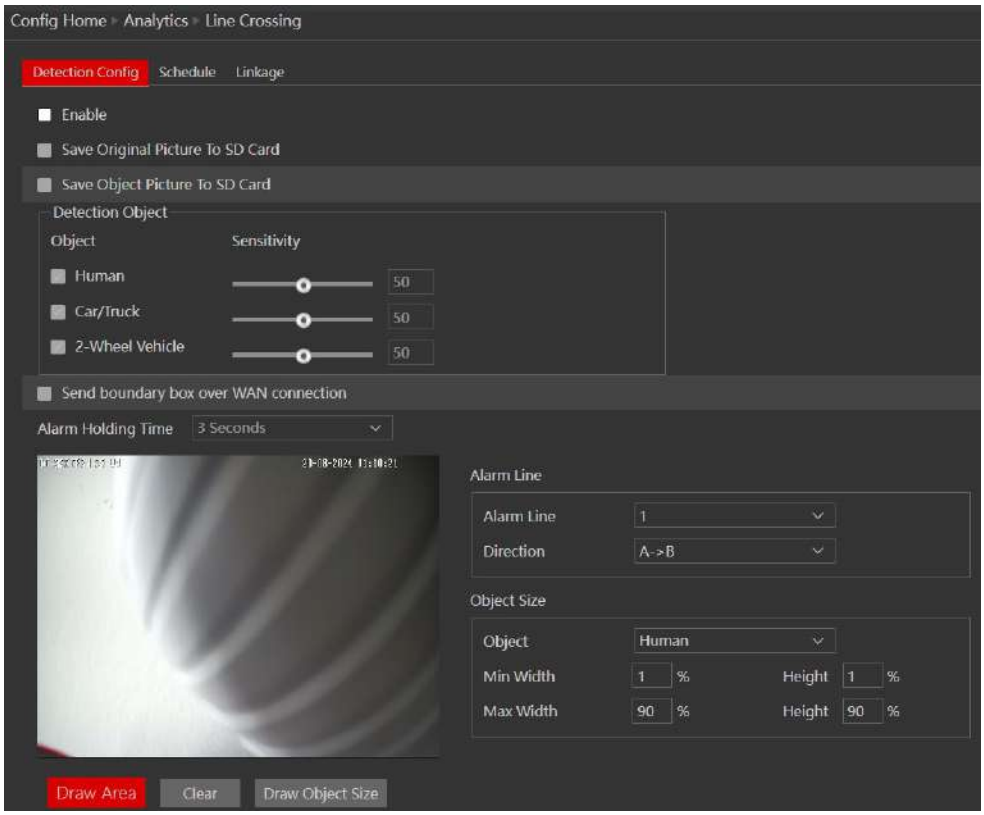
This camera offers advanced video analytics that was designed to detect special scenarios and events. This video analytics detection is based on true object detection of 3 classes: Humans, 4-wheel vehicles, and 2-wheel vehicles. v5.1 offers a variety of Analytics based on Object detection (Line Crossing, Sterile Area) together with other general analytics such as Camera Tampering

Note that some features might not be available in specific models. For confirmation please refer to the camera's technical specs.

5.6.1) Line Crossing

Line Crossing Analytics will detect if a defined object crossed a defined line. The crossing direction can be adjusted.

1. Go to "Advanced Analytics"→ "Line Crossing" to get to the interface as shown below:
2. Enable the Alarm if required.
3. Set whether to save the original picture or the object picture
4. Set the alerting objects and detection sensitivity (Objects not marked will be ignored)



5. Now you will have to set the detection area (lines). Click on the "Area" tab to get to the interface shown below.

6. Click on “Draw Area”.
7. Draw the line. The length of the line should be as long as possible to increase the detection efficiency.
8. Set the crossing direction. The “A” and “B” sides will reflect on the image on the left. The available options are. A→B – Crossing from A side to B side, B→A - Crossing from B side to A side, A<->B – Crossing from any side to any side.
9. Click “Save” to confirm the settings.
10. You can set up to 4 lines. If you wish to set additional lines, change the cordon number and repeat stages 6-9.
11. Set the object minimum and maximum size according to the installation conditions and requirement. Note that you need to set the object size for all object types (Human, Car/Truck, 2-Wheel Vehicle).
12. Next, you will need to set the schedule. Click on the “Schedule”.
13. Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add the required dates to it. The holiday schedule overtakes the normal schedule.
14. Choose the camera’s response to the alarm in the linkage tab as explained below:

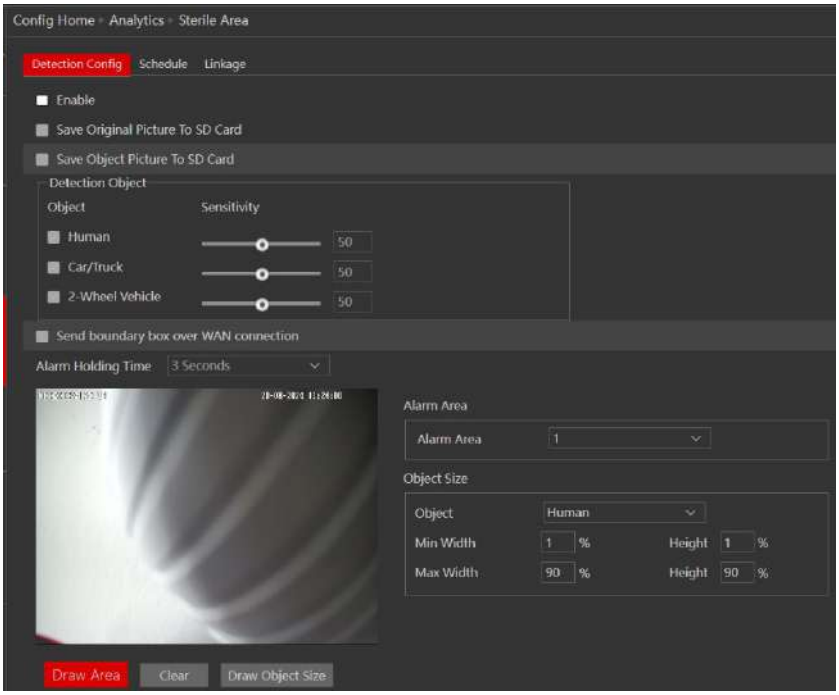
Alarm Triggers:	**Explanation:**
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

15. Click “Save” to save the settings.

5.6.2) Sterile Area

Sterile Area Analytics will detect if any defined object entered the defined area.

1. Go to “Advanced Analytics”→ “Sterile Area” to get to the interface as shown below:
2. Enable the Alarm if required.
3. Set whether to save the original picture or the object picture



4. Set the alerting objects and detection sensitivity (Objects not marked will be ignored)
5. Now you will have to set the detection area. Click on the “Area” tab to get to the interface shown below.
6. Click on “Draw Area”.
7. Draw the area. Drawing the area is done by clicking on the corners of the area you wish to monitor. The maximum points for the polygon are 6. Once you marked the 6th corner, the camera will automatically connect it with the 1st point and close the area.
8. Set the object minimum and maximum size according to the installation conditions and requirement. Note that you need to set the object size for all object types (Human, Car/Truck, 2-Wheel Vehicle).
9. Click “Save” to confirm the settings.
10. You can set up to 4 areas. If you wish to set additional areas, change the alarm area number and repeat stages 6-8.
11. Next, you will need to set the schedule. Click on the “Schedule” tab to get the following interface:
12. Set the active alarm time for each of the weekdays. You can also set a holiday schedule and add the required dates to it. The holiday schedule overtakes the normal schedule.
13. Choose the camera’s response to the alarm in the linkage tab as explained below:

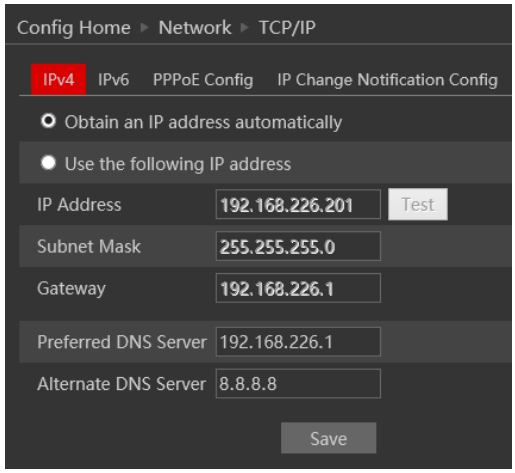
Alarm Triggers:	Explanation:
Trigger SD Card Snapshot	takes a snapshot (SD card must be available)
Trigger SD Card Recording	Initiates video recording over the SD card (SD card must be available)
Trigger Email	sends an email as configured in the Email section.
Trigger FTP	send a snapshot as configured in the FTP section

14. Click “Save” to save the settings.

5.7) Network

5.7.1) TCP/IP

Go to “Network”→ “TCP IP” tab to see the interface shown below. The first and default tab is IPv4 Protocol. There are two options for IP setup: obtain an IP address automatically by DHCP or a defined IP address. You may choose one of the options as required.



DHCP (Automatic IP Assignment): Use “Obtain an IP address automatically” for the camera to communicate with an available DHCP server that will assign the camera with an IP address automatically.

Please note:

- For the DHCP mode to work, you must have a DHCP server on your network.
- Using DHCP for permanent installations is not advisable as the IP Address might change after a while and cause the camera to be unreachable.

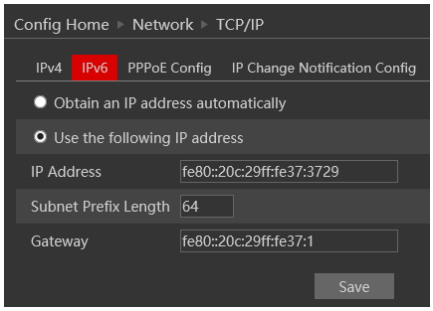
Manual IP Assignment: If you wish to set static IP addresses, choose “Use the following IP Address”, set the range of IP addresses you wish to assign (First and last address), set the gateway and subnet mask, and click on batch set. Wait for a few moments until the IP manager will configure the cameras. After configuration, the IP addresses of the cameras will refresh automatically.

Please note:

- The selected IP address must be available

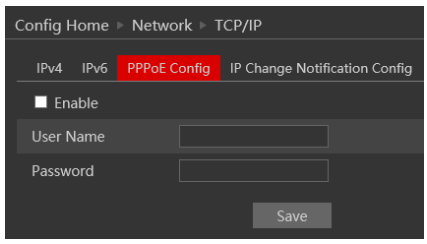
The next tab is IPv6:

If you need to use IPv6, configure it in the same method as described for IPv4.



The next tab is PPPoE:

For PPPoE, the user is required to manually input the username and password for dial-up internet. After saving the username/password information set up an IP address change notification. Last, connect with Modem and the device will dial-up internet automatically.

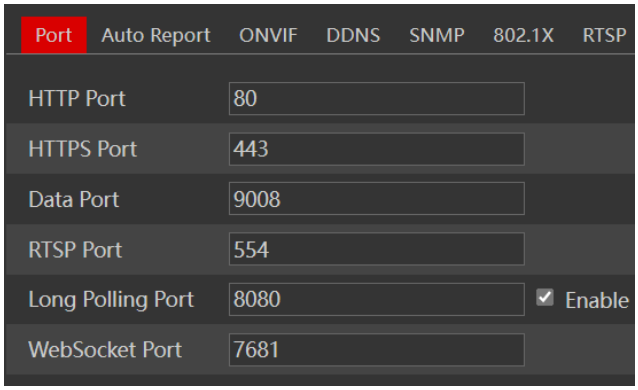


Press the “Save” button to save the settings.

The next tab is “IP Change Notification Config”: If you have used DHCP and you need to be notified that the IP Address assigned to the camera was changed, enable it and set Email or FTP for the notification process.

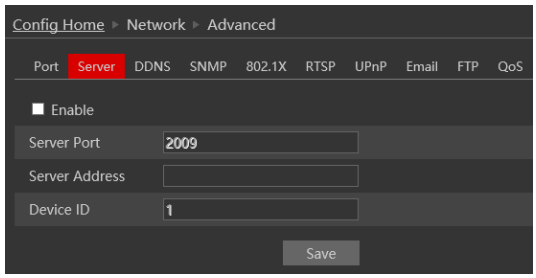
5.7.2) Port

Go to “Network”→ “Port” to see the following interface:



1. HTTP Port (Default is 80) is for HTTP and API
2. Data Port (Default is 9008) is for IE video data and SDK
3. RTSP Port (Default is 554) is for RTSP video streaming
4. Long Polling Port (Default is 8080) is for advanced integrations using long polling API.
5. WebSocket Port (Default is 9681) is for modern browser video streaming

5.7.3) Auto Report



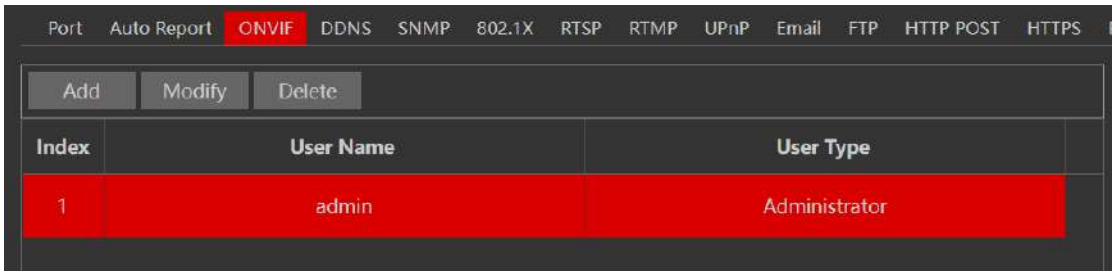
This section refers to “Auto Report Server”. Enable it if required.
Auto report server will make the camera report back to the defined server using port 2009.

Go to “Network”→ “Auto Report”.
Set the port (default port is 2009. It is advisable not to change it.) Set the server address (usually it is the CMS address which needs to be a static address). Set a unique device ID. Each of the devices using auto server report should have its unique ID.
The Camera will report back to the defined server its current IP using port 2009.

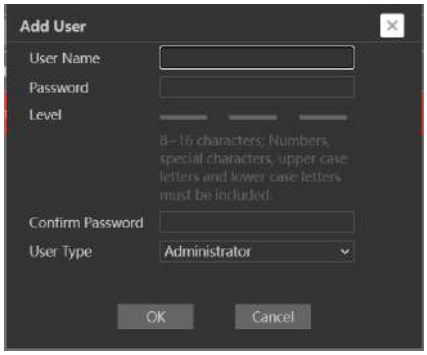
5.7.4) ONVIF

This is the ONVIF management interface. From here you can enable/disable ONVIF and also manage ONVIF users that can be differentiated from the standard IPC users.

Go to “Network”→ “ONVIF” to see the following interface:



If there are no available users, it means that ONVIF is disabled. To enable it, click on “Add”. The following interface will pop up:



Set the username, password, and user type for the required user and click OK.

5.7.5) DDNS

DDNS should be used when your ISP (Internet Service Provider) provides you with a dynamic valid IP. The DDNS will update your dynamic address and link it to a fixed domain.
Enter into the "Network"→"DDNS" tab and set the DDNS as required.

5.7.6) SNMP

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. To Enable and work with SNMP, you need that the switch or another server on the network will support this protocol as well. Though our IPC fully supports SNMP V1/2/3, we will not explain how to configure it in this manual.

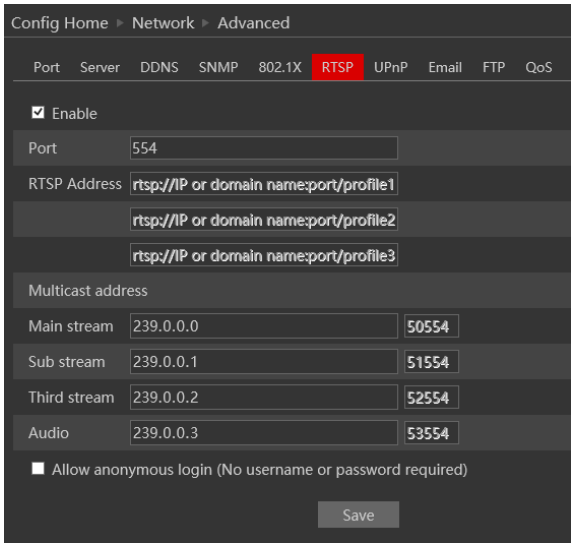
5.7.7) 802.1X

The 802.1X standard is designed to enhance the security of wireless and local area networks (WLANs) that follow the IEEE 802.11 standard. 802.1X provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority.

5.7.8) RTSP

RTSP is used to stream video/audio using the shared protocol. v4.2 is also supporting RTSP using Multicast protocol.

Go to “Network”→ “RTSP” interface as shown below.

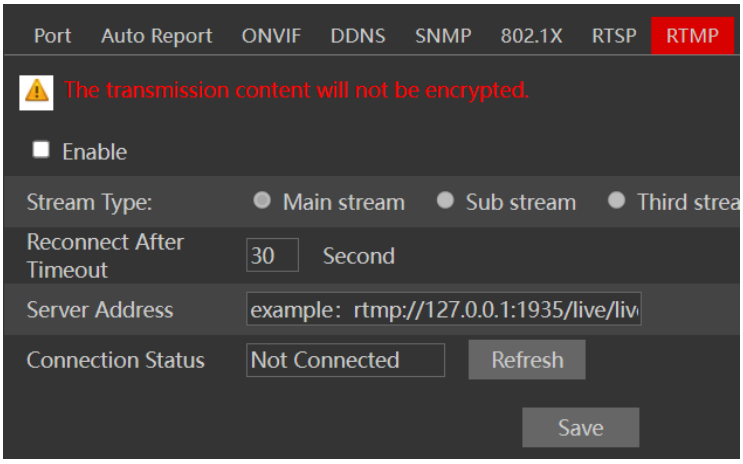


1. Enable the RTSP if required.
2. RTSP Port: Access Port of the streaming media. The default port is 554.
3. RTSP Address: each of the streams has a unique RTSP address. Input the desired address into your RTSP player.
4. Notice that the camera also supports multicast addresses that can be used as well for supporting players.
5. Enabling “Allow anonymous login” will authorize RTSP connection without the need for a username/password.
6. Click “Save” to confirm and save settings.

5.7.9) RTMP

Real-Time Messaging Protocol (RTMP) is a communication protocol for streaming audio, video, and data over the Internet.
Unlike RTSP, once RTMP is configured, the camera will commence video streaming to the configured server as long as it is online.

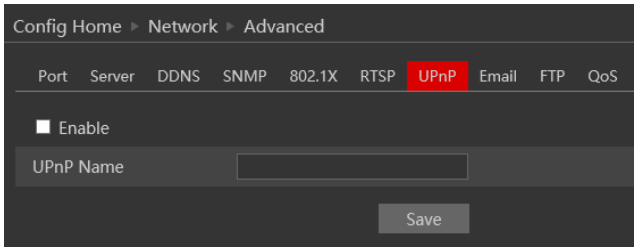
- Go to "Network"→ "RTMP" interface as shown below



- Enable if necessary
- Set the video stream type (Main/Sub/Third-Stream)
- Set reconnection time
- Set the server address. Confirm that the server is listening at the specified address, otherwise, the status will remain "Not Connected"

5.7.10) UPnP

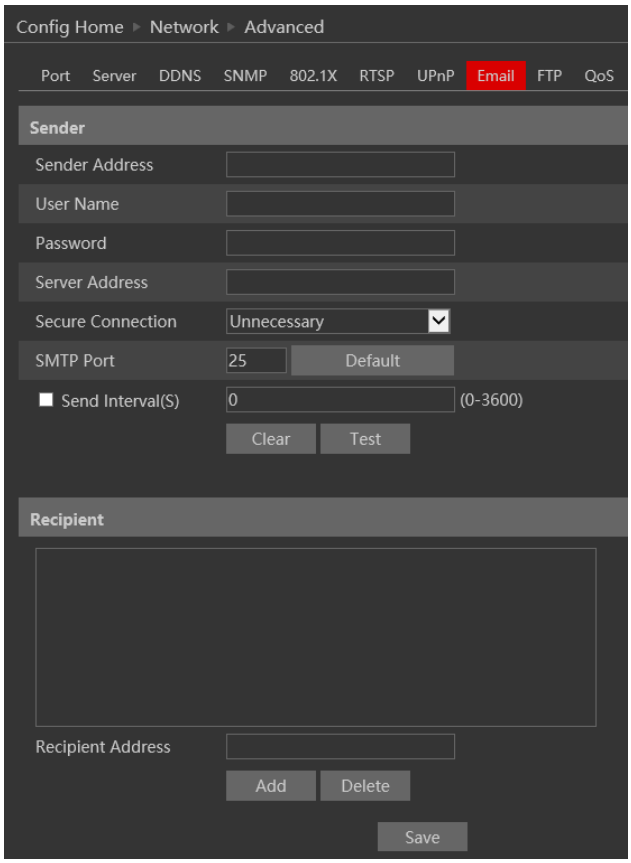
Go to "Network"→ "UPnP" interface as shown below.
Select "Enable UPnP" and then input a friendly name.



Then double-click the "Network" icon on the desktop of the PC to see an icon with the name and IP address of the camera. You may quickly access the device by double-clicking this icon.

5.7.11) Email Setting

Go to “Network” → “Email” interface.



The input fields are as follows:

Field	Meaning
Sender Address	Sender’s e-mail address
User Name	The username of the Email account
Password	The password for the Email account
Server Address	The SMTP/Outgoing Email server address
Secure Connection	Choose between Unnecessary/SSL/TLS
SMTP Port	The SMTP port. The default port will be used according to the secure connection choice but can be edited manually if required.
Send Intervals	The minimum time duration between 2 Emails that will be sent by the system,
Recipient Address	The email addresses that Emails generated by the system will be sent to.

After all the parameters are properly set up, you can click “Test” to confirm that the system can connect to the email server with the provided details. If an email is sent successfully, a “Test Successful” window will pop up, if not, you should try other email addresses or check and correct the settings.

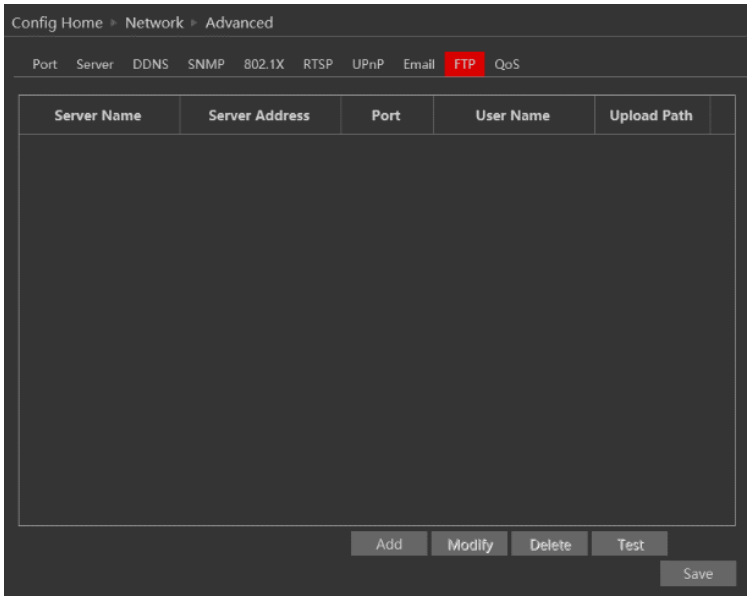
To input a new mail recipient, input the recipient address and click on “Add”. The new address will be added to the recipient list box.

Please note:

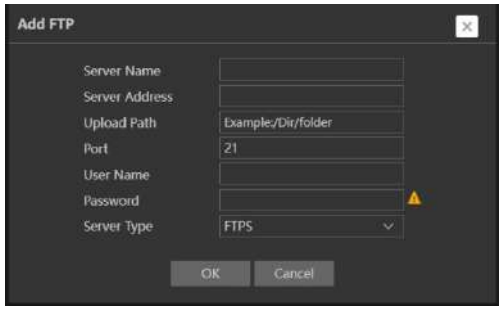
- If you change the static IP into PPPoE and select mailbox, there will be an e-mail sent to your mailbox for notifying a new IP address

5.7.12) FTP

Go to “Network” →”FTP” interface as shown below.



To add a new FTP server click on “Add” and input the FTP server’s server name, address, port number, username, password, and upload path. Set the server type (FTP/FTPS)
Click OK to confirm the setting.



Click on “Modify” to edit the information on the FTP server
Click on “Delete” to delete the FTP server
Click on “Test” to confirm the setting and availability of the FTP server.

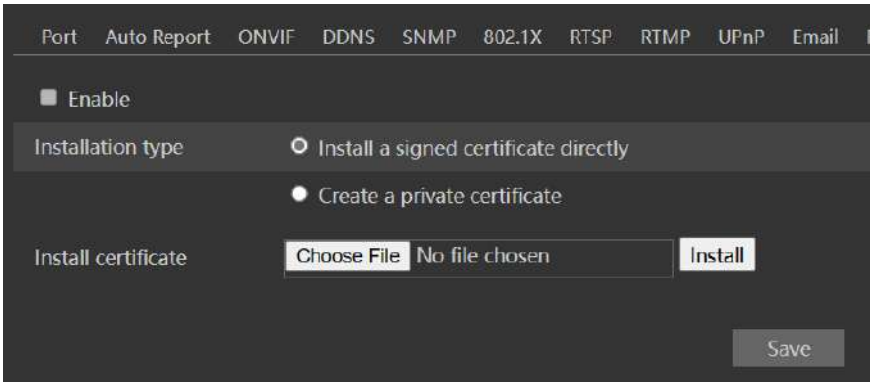
5.7.13) HTTP POST

HTTP POST is used mainly for system integrations. Once enabled, the camera will send **AI events only** to a dedicated listening server. These events will be sent in a detailed XML format that needs to be parsed by the server.
If required, a heartbeat can be set to confirm that the server that the camera is working and has network connectivity to it.

5.7.14) HTTPS

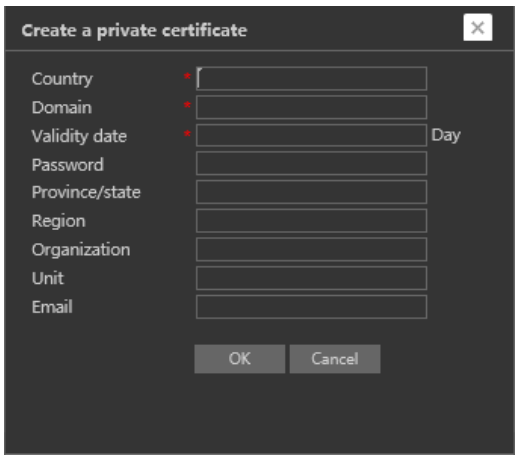
HTTPS (Secured HTTP) is used to establish a secured and encrypted connection between the camera and the client (IE in our case). This will prevent anyone on the network to be able to get information packets and other information by sniffing the network.
The HTTPS must have an SSL certificate to work properly. An authentic certificate must be created by an authorized SSL certificate provider. This will confirm its security and validity. (The internet browser will authenticate the certificate when connecting to the camera).

This is a brief explanation of the SSL certificate and HTTPS connection.
Go to "Network" →"HTTPS". interface as shown below. Enable HTTPS if required. (Enabling HTTPS completely disables HTTP connection).



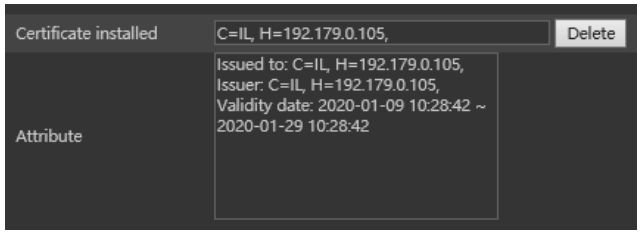
If you already have an SSL certificate in hand, choose "Install a signed certificate directly". Click on "Browse" and choose your certificate. Click on "Install", wait for the procedure to complete, and click on "Save"
If you wish to use a basic HTTPS connection, click on "Create a private certificate". The interface will update to: Create a private certificate Create .

Click on "Create". The interface below will appear.



Input the details (The country field is set by 2 capital letters. For example for Israel the user should input "IL"). The fields marked with * are mandatory. All the rest are optional.

Click on “OK”. Once the procedure is finished, the SSL certificate will be automatically installed as follows.

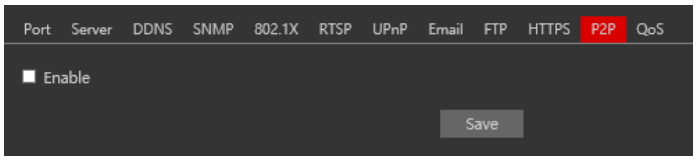


Please note:

- Using this method will display an error message by the browser every time you connect to the camera, as the camera is not recognized as a certified SSL certificate issuer.

5.7.15) P2P

P2P is used to connect directly to the camera through an advanced NAT interface.
Go to “Network” →”P2P”.



Enable P2P if required.
Once enabled you can refer to “Settings”→”System”→”Basic Information”

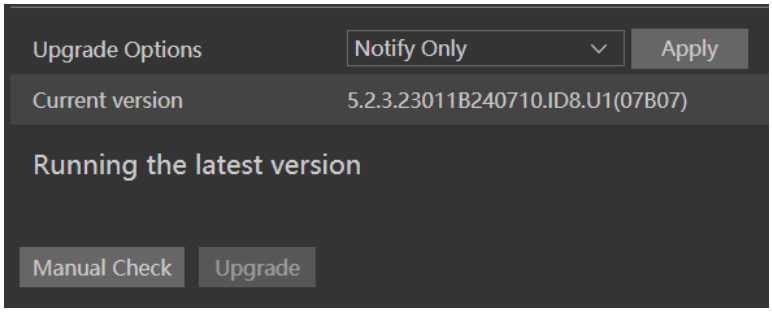
Scan the QR code using the “Provision Cam2” mobile APP or input the device ID manually in the P2P domain (https://www.provisionisr-cloud.com).

5.7.16) QoS

Quality of Service (QoS) is an advanced feature that prioritizes internet traffic for applications to minimize the impact of busy bandwidth. It must be supported by the switch/router being used.

5.7.17) Cloud Upgrade

Cloud upgrade is used to update the camera remotely using OTA (Over The Air) update technology. Enable it by setting the “Upgrade Options” to “Notify Only”. The IPC can be then updated manually through the web UI, through the Provision Cam2 App, or through the NVR.

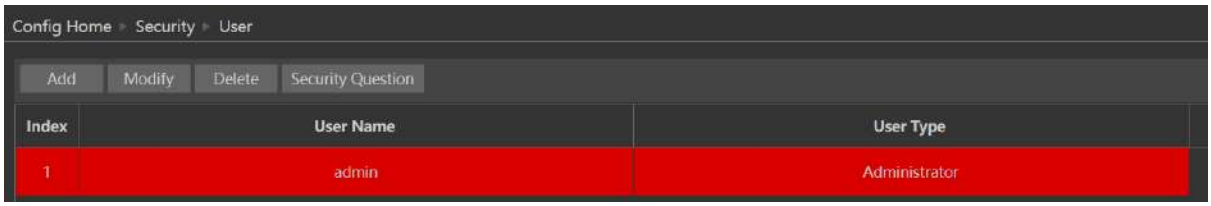


5.8) Security

Security configuration includes three submenus: User Settings, Online Users, and Block & Allow lists.

5.8.1) User

Go to "Network" →"User" to access the following interface.



Adding a user:

Click on the "Add" button to pop up the "Add user" dialog box.

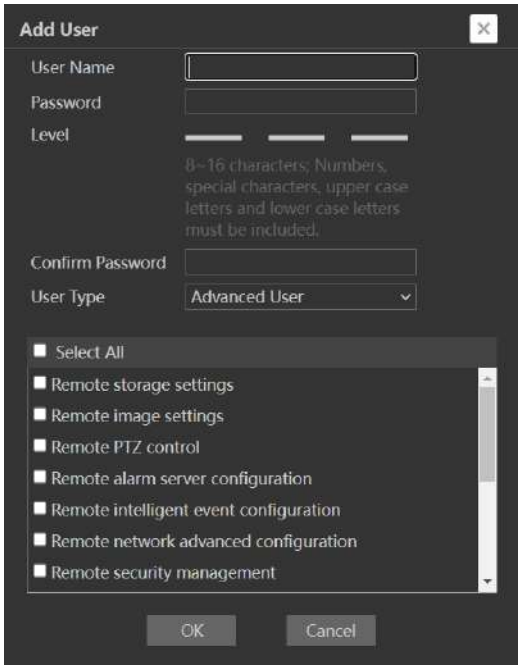
Input the username, and password and confirm the password.

Set the user type. 3 user types are available:

- Administrator – Can perform all actions and settings on the camera.
- Advanced user – Can view and configure the camera excluding the "User Access" section.
- Normal User – Can only view the live image and cannot configure.

At this stage, you can also bind a MAC address for the user. This means that this user will only be able to connect from a single pre-defined device and his access will be denied if he will try to connect from any other device.

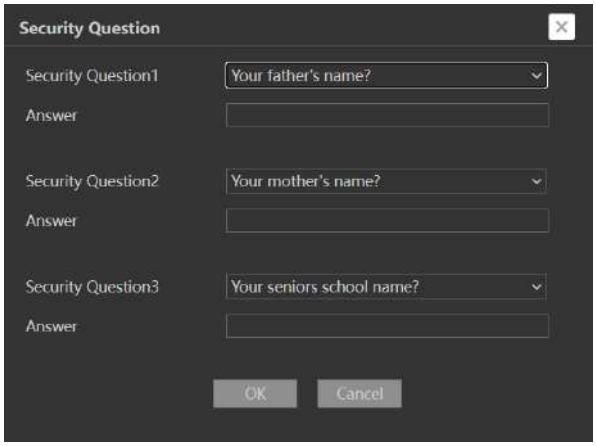
Click on "OK" and "Save"



Modify user:
Select the user you wish to modify and click on the “Modify” button. A modification window will pop up as shown above.
You can change the username if required. If you wish to edit the password of the user, tick “modify password” and input the old password, new password, and confirmation of the new password.
Click “OK” to save.

Delete user:
Select the user you wish to delete and click on the “Delete” button. A confirmation prompt will pop up. Click “Ok” to confirm.

Editing the Security Questions:
If you wish to set/edit the security questions used to recover your admin password, you can do so by clicking on “Security Question”. The following window will pop up:
Choose 3 questions from the drop-down list and set the correct answers. Note that when recovering a lost admin password, **all** questions should be answered correctly

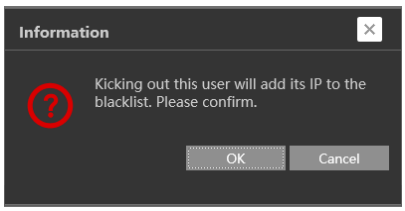


5.8.2) Online Users

The “Online users” section will allow you to view users who are currently connected to the camera. Administrator-level users can also kick out other users who are currently connected to the camera.
Go to “Network” →“Online Users” to access the following interface.

You can view the IP address, port, username, and user type used for the connection.

The “Kick Out” button will kick out the selected user and input his IP address to the blacklist. Click on it for the relevant user and confirm the prompt message.



Please note:

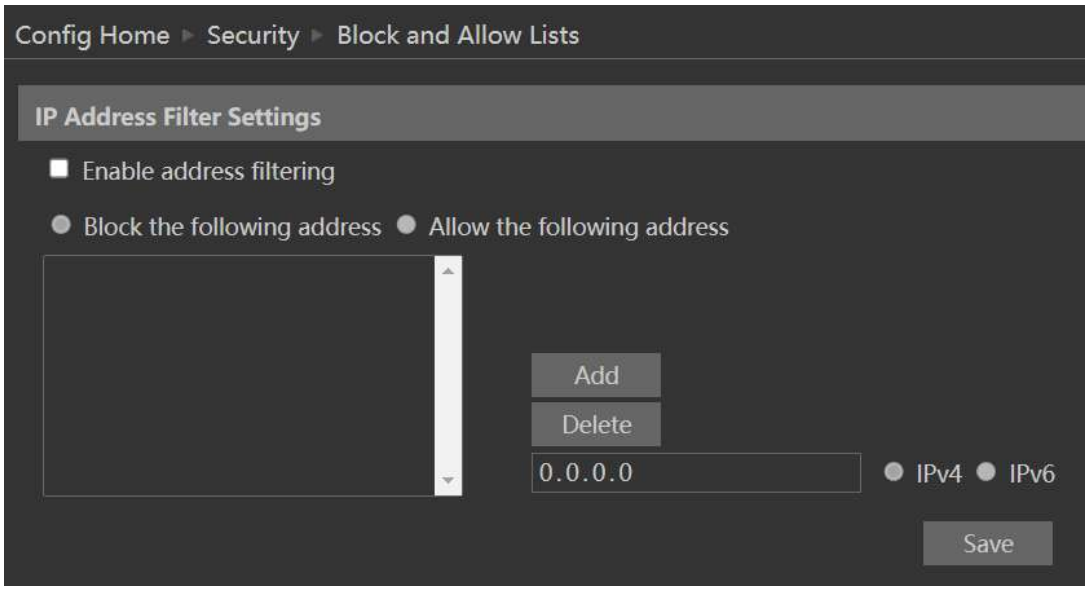
- Once the user is kicked out, the IP address used for the connection will be blacklisted. Therefore, the device used for connection will not be able to connect to the camera until the IP address will be manually removed from the blacklist.

5.8.3) Block and Allow Lists

"Block and Allow" lists allow the user to create lists of IP/MAC addresses that will be allowed or denied for connection.

Once a "Block" list is created, all devices except the blocked devices will be allowed to connect to the camera.
Once an "Allow" list is created, all devices except the allowed devices will be blocked from connecting to the camera.

Go to "Network" →"Block and Allow Lists" to access the following interface.



The lists can be based on IPv4/IPv6.

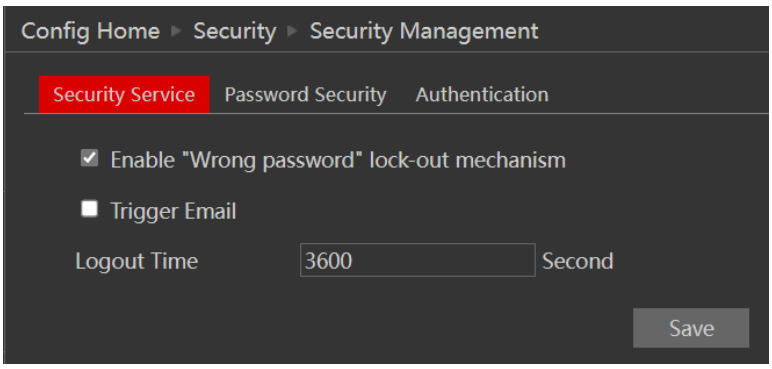
Enable the filtering you wish to activate.

1. Choose the type of list you wish to create (block or allow)
2. Set whether the input is IPv4/IPv6 address
3. Input the IP address you wish to add to the list
4. Click on add.
5. If you wish to add more than one address, repeat stages 1-4
6. Once finished, click "Save" to confirm, save the settings, and enable the lists.

5.8.4) Security Management

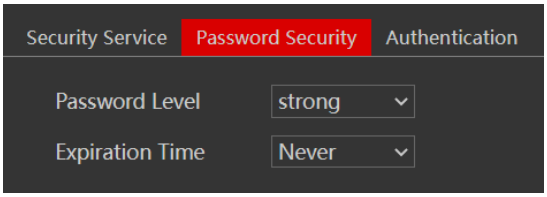
"Security Management" Allows the user to enhance the device security by adding protection layers and rules.

"Security Service" enables a mechanism that locks the IPC to an incoming connection after 5 wrong attempts. Releasing the camera from a locked state is done by waiting for the lock duration or hard rebooting the camera. This mechanism protects against a "Brute Force" attack.



Ticking the "Trigger Mail" will send a mail to the selected recipients notifying them that the camera entered a "lock" state due to multiple failed login attempts.

"Password security" allows the user to set the password required strength and password change policy.

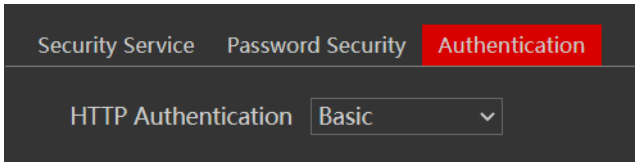


Password level divides into 3 levels:

- Low: No Requirements.
- Mid: Minimum of 8 characters. Contains at least one number and one character.
- High: Minimum of 8 characters. Contains at least one number, one character, and one special character.

Expiration time: After the set duration (30 Days, 60 Days, Half a Year, Year), the camera will demand a password change. The current password cannot be reused. Older passwords are not kept and can be used again.

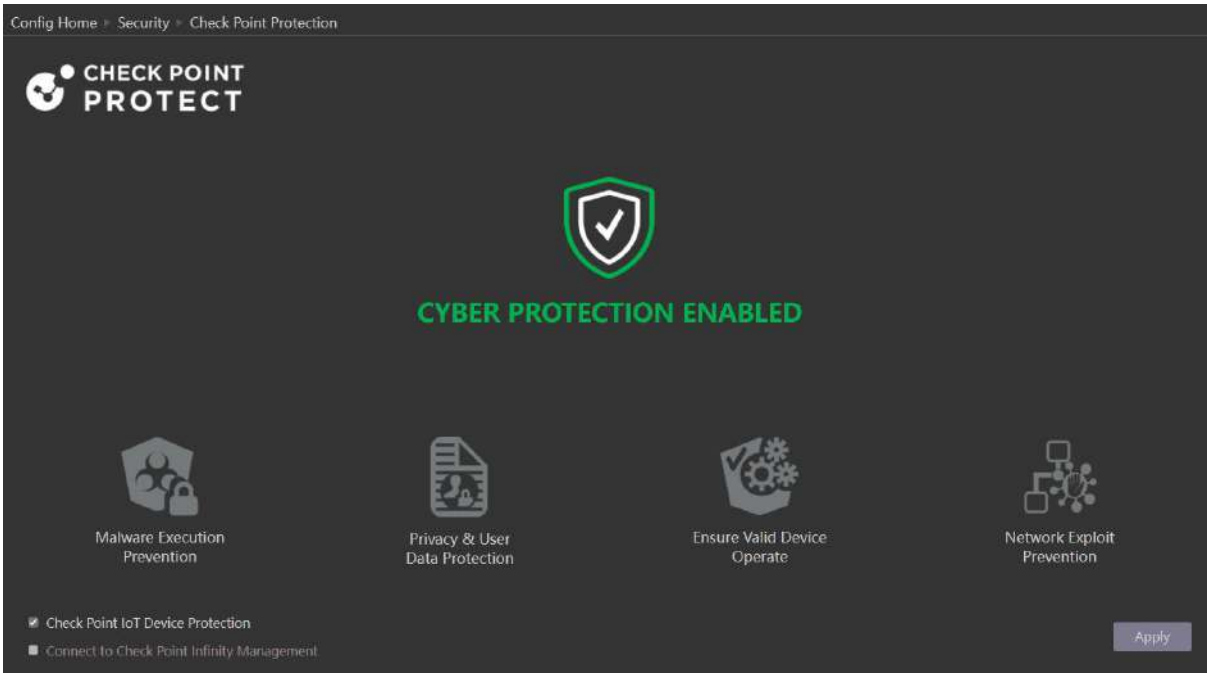
"Authentication" is used for API HTTP login.
"Basic" is Base64 authentication, and "Token" is digest MD5 authentication.



5.8.5) Check Point Protection

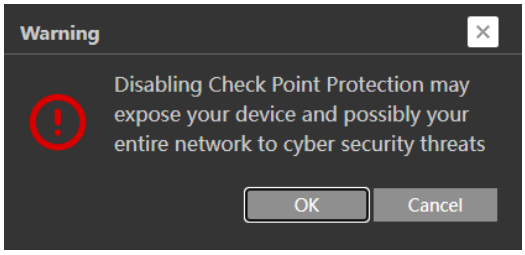
Check Point IoT Protect Nano agent is a dedicated real-time runtime cyber protection layer provided by Check Point®.

Click on Settings→Security→Check Point Protection to open the following interface:



Disabling the protection:

1. Untick "Check Point IoT Device Protection"
2. The following message will pop up



3. Confirm that you wish to proceed.
4. Click "Apply"
5. Input the admin password and confirm again.

Please note:

- It is highly advised to keep the IoT Protect enabled at all times.
- Disabling Check Point protection may expose your device and possibly your entire network to cyber security threats

5.9) Maintenance

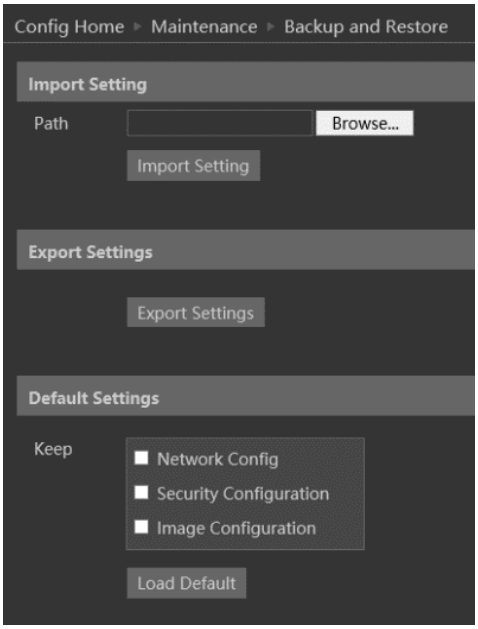
Maintenance includes 4 submenus: Backup & Restore, Reboot, Upgrade, and Operation log.

5.9.1) Configure Backup & Restore

Backup and restore are used to save the camera's configuration on a PC and use it in case the camera's configuration was changed or when you wish to change the configuration of several cameras to be uniform. This section also allows you to restore the camera's setting to factory default with some exceptions.

Go to "Maintenance"→" Backup and Restore".

Importing Settings: If you have a configuration file and you wish to import it to the camera, click on "browse" and choose the relevant config file.
After choosing the file click on "Import settings" and wait for the process to finish.



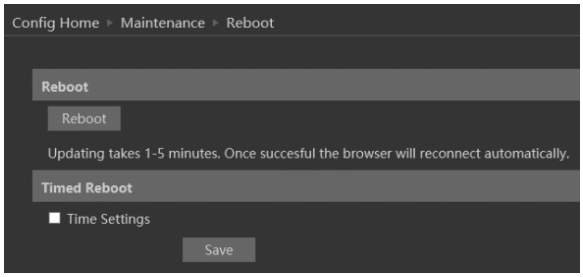
Exporting settings: If you wish to export the configuration settings of the camera click on "Export". Choose the location on your PC and set the file name. Click on "OK" to save the file in the desired location.

Loading factory default: If for any reason you wish to restore your camera settings to factory default, you can use the "Load Default" button. Notice that you can mark some configurations that will be saved:

- Network Config: Will save all the network section configuration
- Security Configuration: This will save all the security section configurations.
- Image configuration: Will save the image section configuration.

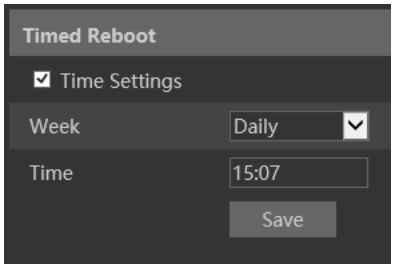
5.9.2) Reboot Device

Go to "Maintenance"→"Reboot" to see the interface as shown below.



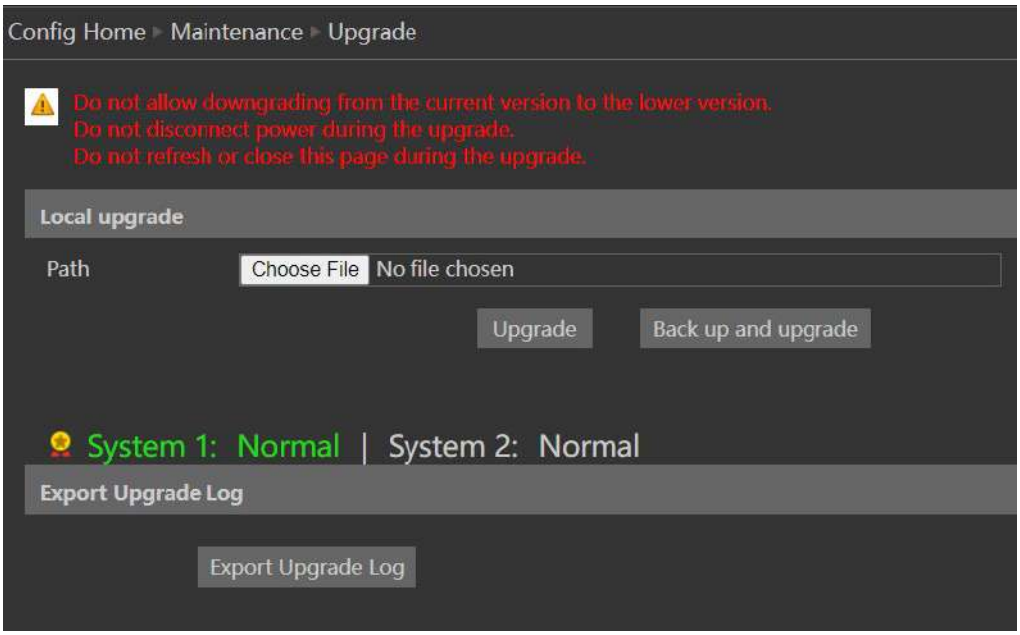
To reboot the IPC, click on the reboot "Reboot" button and confirm the pop-up prompt message, then wait for the reboot process to finish.

You can also set a scheduled reboot. Tick the “Time Settings” and set the time period and time for the reboot. You can choose a day of the week when the reboot will automatically take place or you can set it to happen daily. The reboot will occur on the specified day and time.



5.9.3) Upgrade

Go to “Maintenance”→”Update” to open the interface as shown below.



1) Click the “Browse” button to select the upgrade file.
2) Click the “Upgrade” button to start the upgrading process of the IPC.
3) The device will restart automatically once completed.
4) Depending on the update release note, the IPC configuration might reset.

Please note:

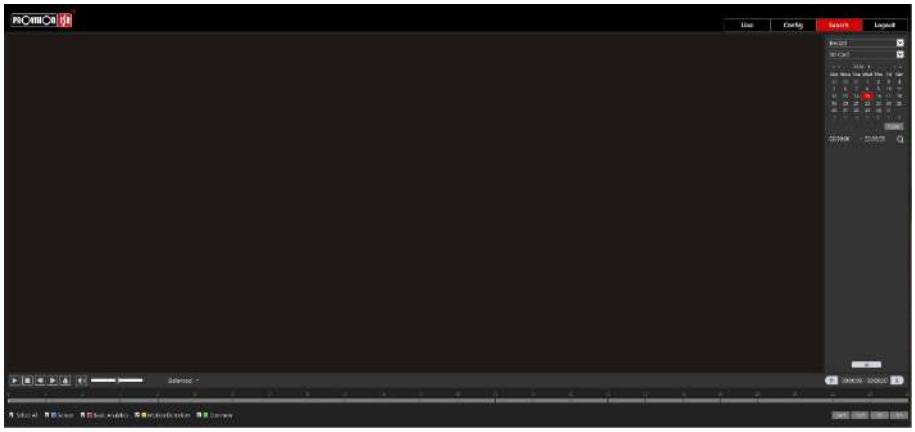
- You must not disconnect to PC or close the IPC during the upgrade process to prevent permanent damage to the camera.
- If the camera update file is ***.TAR. the “TAR” file should not be extracted.
- After an update, the camera will enter “Ebservation mode” for 10 minutes to confirm the update integritiy and the normal operation of the camera. During this time, the camera cannot be updated again.

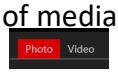
6) Playback

Playing back videos taken by the camera have 2 options:

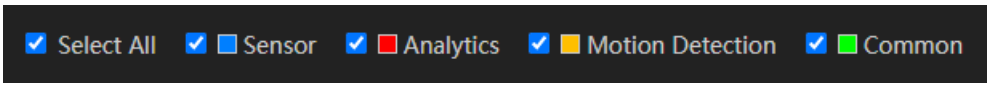
1. Video files/Images saved locally on the PC (If any were taken)
2. Video files/Images saved on the Camera SD card (If available)

To access the playback interface, click on the “Search” Main tab. The interface below will appear.

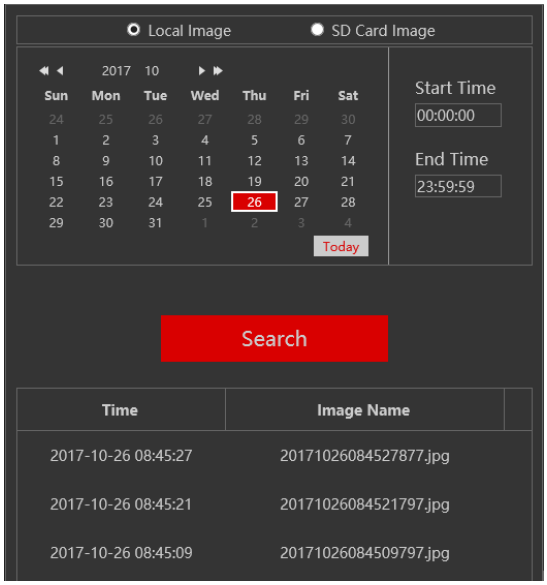


1. First, you will have to choose which type of media you wish to search for. On the left top corner choose from Photo and Video 

2. Choose the location of the stored media. You can either choose “Local” – which is your PC or you can choose “SD Card” which is the camera’s internal SD Card.
3. If you chose the SD card as the search source you can also define the alarm trigger as follows:



4. Set the search range. You can choose a single day and set a time range of up to 24 hours. (Full day). Once finished click on “Search” to show the results.



5. Double-click on the image/video from the list for it to show on the main playback window and to the playback queue.

6. The playback controls are described below. Notice that it is different for Videos and Photos

For Photos

Icon	Description	Icon	Description
	Close the displayed image		Digital Zoom In
	Close the displayed image and delete the queue list		Digital Zoom out
	Download the displayed image to your PC (SD Card search only)		Play a slideshow of the queued images
	Download the displayed image and queue list to your PC (SD Card search only)		Stop the slideshow
	Fit the image to the screen	2.5S	Dwell time between images
	Display the image in real-size		

For Videos

Icon	Description	Icon	Description
	Play		Play next file
	Pause playback		Enable/Disable Watermark
	Stop Playback		Download the selected file (SD Card only)
	Reduce playback speed		Enable/Disable Audio + Volume control
	Increase playback speed		Full-screen mode
	Play the previous file	Balanced	Buffering mode selection

Provision-ISR
11 Atir Yeda St, Kfar Saba,
Israel
Postal Code: 4442510
Tel: (972-9) 741 7511
Web: www.provision-isr.com